

Please type a plus sign (+) inside this box → ☐

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	TI-25667
First Named Inventor or Application Identifier	Roy I. Edenson et al.
Title	Secure Distribution of Digital Data
Express Mail Label No.	EL 008142954 US

APPLICATION ELEMENTS

See MPEP Chapter 600 concerning utility patent application contents

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

- ☒ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original, and a duplicate for fee processing)
- ☒ Specification [Total Pages **25**]
(preferred arrangement set forth below)
 - Descriptive title of the invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R&D
 - Reference to Microfiche Appendix
 - Background of the invention
 - Brief Summary of the invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
- ☒ Drawing(s) (35 USC d113) [Total Sheets **3**]
- Oath or Declaration [Total Pages **2**]
 - ☒ Newly Executed (original or copy)
 - ☐ Copy from a prior application (37 CFR §1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
 - ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s)
named in the prior application,
see 37 CFR §1.63(d)(2) and 1.33(b).
- ☐ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of
the oath or declaration is supplied under Box 4b, is considered as
being part of the disclosure of the accompanying application and is
hereby incorporated by reference therein.

- ☐ Microfiche Computer Program (Appendix)
- Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
 - ☐ Computer Readable Copy
 - ☐ Paper Copy (identical to computer copy)
 - ☐ Statement verifying identical of above copies

ACCOMPANYING APPLICATION PARTS

- ☒ Assignment Papers (cover sheet & Documents(s))
- ☐ 37 CFR §3.73(b) Statement (when there is an assignee) ☒ Power of Attorney
- ☐ English Translation Document (if applicable)
- ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
- ☒ Preliminary Amendment
- ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
- ☐ Small Entity Statement(s) ☐ Statement filed in prior application
Status still proper and desired
(PTO/SB/09-12)
- ☐ Certified Copy of Priority Document(s)
if foreign priority is claimed
- ☐ Other:

* A new statement is required to be entitled to pay small entity fees, except where one has been filed in a prior application and is being relied upon.

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: /

Prior application information: Examiner _____ Group / Art Unit: _____

18. CORRESPONDENCE ADDRESS

☐ Customer Number or Bar Code Label

(Insert Customer No. or Attach bar code label here)

or ☒ Correspondence address below

NAME	Charles A. Brill		
	Texas Instruments Incorporated		
ADDRESS	P.O. Box 655474, MS 3999		
CITY	Dallas	STATE	TX
COUNTRY	USA	ZIP CODE	75265
	TELEPHONE	FAX	972-917-4418
	972-917-4379		

Name (Print/Type)	Charles A. Brill	Registration No. (Attorney/Agent)	37,786
Signature	Charles A. Brill	Date	10/12/98

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL

Patent fees are subject to annual revision on October 1.

These are the fees effective October 1, 1997

Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB/09-12.**Complete If Known**

Application Number	Provisional 60/061,799
Filing Date	Provisional 10/14/97
First Named Inventor	Roy I. Edenson et al.
Examiner Name	TBD
Group / Art Unit	TBD
Attorney Docket No.	TI-25667

TOTAL AMOUNT OF PAYMENT (\$)**1,438.00****METHOD OF PAYMENT**

- 1.
- ☒
- The Commissioner is hereby authorized to charge to the following Deposit Account,

Deposit Account Number

20-0668

Deposit Account Name

Texas Instruments Incorporated

- ☒
- Charge any additional fee required or credit any overpayment

- ☐
- Charge all indicated fees and any additional fee required or credit any overpayment

- 2.
- ☐
- Payment Enclosed:

☐

Check

☐

Money Order

☐

Other

FEE CALCULATION**1. BASIC FILING FEE**

Larg e Fee Code	Entity Fee (\$)	Small Fee Code	Entity Fee (\$)	Fee Description	Fee Paid
101	790	201	395	Utility filing fee	\$790
106	330	206	165	Design filing fee	\$
107	540	207	270	Plant filing fee	\$
108	790	208	395	Reissue filing fee	\$
114	150	214	75	Provisional filing fee	\$

SUBTOTAL (1) (\$)**790****2. EXTRA CLAIM FEES**

Total Claims	Extra Claims	Fee from below	Fee Paid
42	-20**= 22	22	484
Independent Claims	5	-3**= 2	164
Multiple Dependent			

**or number previously paid, if greater; For Reissue, see below

Larg e Fee Code	Entity Fee (\$)	Small Fee Code	Entity Fee (\$)	Fee Description
103	22	203	11	Claims in excess of 20
102	82	202	41	Independent Claims in excess of 3
104	270	204	135	Multiple dependent claims in excess of 3
109	82	209	41	**Reissue independent claims over original patent
110	22	210	11	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) (\$)**648****FEE CALCULATION (continued)****3. ADDITIONAL FEES**

Larg e Fee Code	Entity Fee (\$)	Small Fee Code	Entity Fee (\$)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	400	216	200	Extension of time within second month	
117	950	217	475	Extension of time within third month	
118	1,510	218	755	Extension of time within fourth month	
128	2,060	228	1,030	Extension of time within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,320	241	660	Petition to revive - unintentional	
142	1,320	242	660	Utility issue fee (or reissue)	
143	450	243	225	Design issue fee	
144	670	244	335	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt.	
581	40	581	40	Recording each patent assignment per properly (time number of properties)	
146	790	246	395	Filing a submission after final rejection (37 CFR 1.129(a))	
149	790	249	395	For each additional invention to be	

Other fee (specify)

Other fee (specify)

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3)

0

SUBMITTED BY

Typed or Printed Name

Charles A. Brill

Signature

Charles A. Brill

Date

10/12/97

Complete (if applicable)

Reg. Number

37,786

Deposit Account User ID

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Edenson et al.

Art Unit: TBD

Parent Serial No.: 60/061,799

Examiner: TBD

Parent Filed: 10/14/97

Docket No. TI-25667

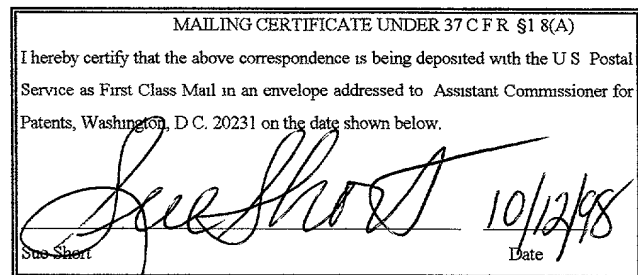
For: SECURE DISTRIBUTION OF DIGITAL DATA

PRELIMINARY AMENDMENT

October 9, 1998

Assistant Commissioner for Patents

Washington, DC 20231



Dear Sir:

In support of the accompanying patent application, applicant amends as follows:

In the specification:

Page 1, prior to the first sentence: Please insert --This application claims priority under 35 U.S.C.

§ 119 (e)(1) of provisional application number 60/061,799 filed October 14, 1997.--

Page 3, line 16: Please delete "there" and substitute therefor --the--.

Page 5, line 5: Please delete "data, and" and substitute therefor --data and--.

Page 5, line 6: Please delete "medium, the" and substitute therefor --medium. The--.

Page 5, line 6: Please delete "containing" and substitute therefor --contains--.

Page 5, line 14: Please delete "containing" and substitute therefor --contains--.

Page 5, line 14: Please delete "indicate" and substitute therefor --indicating--.

Page 7, line 11: Please delete "processed" and substitute therefor --performed--.

Page 9, line 9: Please delete "RF module interrogator" and substitute therefor --identification module interrogator--.

Page 9, line 21: Please delete "The lower" and substitute therefor --To lower--.

601061799-101398

REMARKS

Consideration of the present application is respectfully requested.

Respectfully submitted,



Charles A. Brill
Reg. No. 37,786

Texas Instruments Incorporated
PO Box 655474 M/S 3999
Dallas, TX 75265
(972) 917-4379
FAX: (972) 917-4418

0607-430260

SECURE DISTRIBUTION OF DIGITAL DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

The following patents and/or commonly assigned patent applications are hereby incorporated herein by reference:

5	Patent No.	Filing Date	Issue Date	Title
	5,053,774	Feb. 13, 1991	Oct. 1, 1991	Transponder System
	08/850,535	May 2, 1997		A TIRIS Based Kernel for Protection of Copyrighted" Program Material
10	60/033,543	Dec. 20, 1996		A TIRIS Based BIOS for Protection of "Copyrighted" Program Material
	60/048,266	June 2, 1997		Data Protection System

FIELD OF THE INVENTION

This invention relates to the field of data distribution systems, more particularly to methods and systems for distributing recorded digital data, still more particularly to methods and systems for distributing digital electronic cinema data recorded on optical discs.

BACKGROUND OF THE INVENTION

Motion picture film no longer is a convenient medium by which to distribute video information. Producing copies of a film is a time consuming process which, while not prohibitively expensive or difficult, is much more expensive than modern alternatives such as manufacturing optical discs. Film is also a relatively heavy medium which, at 25 pounds a canister, represents a significant shipping expense. Film's disadvantages do not end with production and distribution, display of the films requires a trained projectionist to assemble the films with trailers and to operate the projection system. Furthermore, film quickly degrades, often

with more than 80% of the scratches and dirt accumulating on a film within the first two days of release.

In addition to all of the physical drawbacks involved with the use of film to distribute motion pictures, there are also significant security concerns involved with the use of film. These security drawbacks center around the economic structure of the motion picture industry. Motion pictures represent an tremendous investment of capital by the production studios. The production studios rely on a stream of income over an extended period of time to recoup this investment and return a profit. This income stream is fed by admission charges during the initial theater showings of new releases and through various other outlets for older motion pictures such as sales of video cassettes and royalties from television broadcasts.

Unlike many other industries where there are underlying assets such as factories or secret production methodologies which prevent others from competing directly with the original producers of a product, the motion picture industry releases a product that may be easily and cheaply reproduced, or reused, without the necessity of a large capital investment. These reproductions compete directly with the original copies for audiences and markets--without generating additional revenue for the production studios. In the past, these unauthorized reproductions were typically of inferior quality--a trait that limited the demand for the unauthorized reproductions. As motion picture distribution transitions from a photographic-based medium to a digital computer-based medium, however, the unauthorized copies typically will be perfect copies of the original.

Furthermore, since the distribution agreements generally call for a royalty payment based on the number of showings, simply making unauthorized showings of the original also avoids royalty charges. Unauthorized reproductions and additional showings not only deprive the

motion picture studios of royalty income, they also reduce the studio's control over the release and publicity of the movie. Advertising heavily influences the motion picture viewing public. The motion picture industry carefully orchestrates the release of each picture to coordinate the distribution with the associated advertising campaign. Box office receipts control the amount of advertising a particular film receives, as well as the number of screens which will show the film. Furthermore, films almost always are released in the United States first, since it is the largest market, and released in other countries several weeks, or often months, later. Unauthorized copies generated from U.S. versions of a film sometimes are shown in foreign theaters as little as one week after the U.S. release date.

Intellectual property laws protect producers of valuable technical and creative information. Specifically, copyright laws are designed to protect the content of motion pictures from unauthorized duplication and performance, both in the United States and internationally. In spite of the protection available through intellectual property laws, motion picture producers have been vulnerable to copyright infringement both in the United States and abroad. This infringement may be perpetrated by the motion picture distributor, theater owner, or even an independent party who gains access to the film. Therefore, there motion picture industry is in need of a system of distribution that improves the security of the motion picture content.

SUMMARY OF THE INVENTION

It is a primary object of the present invention to provide a system and method of distributing digital data which provides data security through a multi-tiered system of safeguards. According to one embodiment of the disclosed invention, a secure digital image projection system is provided which has at least one identification code identifying the image projection system, and comprises: an identification system interrogator for reading an authorization code from an identification system module associated with a data storage medium, a verification unit for verifying the authorization code matches the identification code, a reader for reading digital data stored on the data storage medium, and a projection engine for displaying the digital data on the condition that the authorization code matches the identification code. Examples of identification systems include an RF identification systems and a Texas Instruments Registration and Identification System (TIRIS®) transponder. Variations on this embodiment include systems utilizing encrypted data, compressed data, separate media players and projectors, and tamper-proof cartridges enclosing the storage media.

According to another embodiment of the present invention, a secure digital data media player is disclosed. The secure digital data media comprising: an identification system interrogator for reading authorization information from an identification system module attached to a digital data storage medium and verifying the authorization information authorizes the media player to read the digital data storage medium, and a media reader for reading data from the digital data storage medium and outputting the data on the condition the authorization information authorizes the media player to read the digital data storage medium. Examples of identification system modules include an RF identification system module and a TIRIS transponder. Variations on this embodiment include systems utilizing encrypted data, compressed

data, separate media players and projectors, and tamper-proof cartridges enclosing the storage media.

According to another embodiment of the disclosed invention, a secure data storage medium is disclosed. The secure data storage medium comprising: a digital storage medium for storing digital data, and an identification system module corresponding to the digital storage medium, the identification system module containing an authorization code describing which media players are authorized to read digital data from the digital storage medium. Variations to this embodiment include the use of an optical disc, an RF identification system, and a TIRIS responder.

According to yet another embodiment of the disclosed invention, a method of securely distributing digital data is disclosed. The disclosed method of securely distributing digital data comprises: writing digital data onto a digital storage medium, and attaching an identification system module to the digital storage medium. According to this embodiment, the identification system module containing an authorization code indicate which media readers are authorized to read the digital storage medium. Variations to this embodiment include the use of an optical disc, an RF identification system, and a TIRIS responder.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

5 FIGURE 1 is a block diagram of one embodiment of an improved distribution system showing the production of the digital media, the distribution of the media, and the playback of media and projection of the resulting image.

FIGURE 2 is a schematic representation of a three-chip DMD-based projection system.

10 FIGURE 3 is a block diagram of one embodiment of an improved distribution system showing a tamper-proof disc cartridge, and a combined media player and projector.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An improved distribution system has been developed that provides improved image quality, improved media durability, reduced media duplication and distribution costs, improved bookkeeping capability, and dramatically improved security. The distribution system is based on digital recording technologies which enable the use of all-digital image projection techniques.

An all-digital image distribution and projection system provides many advantages over traditional analog or mixed digital-analog systems. First, the all-digital nature of the disclosed distribution and projection system provides a higher level of security than possible using analog techniques. The all-digital distribution and projection system enables the use of encryption and decryption schemes which make intercepted data virtually useless to unauthorized parties.

Second, because all processing necessary to display the digitized movie data is processed in the digital domain, non-linearities, signal cross-coupling, noise degradation, bandwidth limitations, color impurities, temperature variations, and other degrading artifacts often associated with analog display means are eliminated or significantly reduced. Data errors which do occur are detected and corrected through the use of traditional error detection and correction techniques.

The disclosed distribution system is enabled by the rapid advance in digital communication technologies which have dramatically reduced the amount of information necessary to store and create electronic cinema images, advances in radio frequency (RF) identification technologies, and the availability of true digital imaging technologies. Furthermore, the disclosed secure distribution techniques, while widely applicable outside the motion picture industry, are ideally suited to use in motion picture distribution due to the unique characteristics of the motion picture industry. The disclosed distribution system is ideally suited for implementation in the motion picture industry since there is a demand for the highest possible image quality, a relatively small number of display

projectors compared to other markets such as home theater or television, and because of the high cost of existing media duplication and distribution techniques.

Figure 1 is a block diagram of the improved distribution system showing production of the digital media 102, distribution of the media 117, and playback of media 118 and projection of the resulting image 128. The disclosed data distribution system uses storage media 114, typically optical storage media, which has been coupled with a tamper-proof identification system. The optical data storage medium is preferably a high quality digital optical disk, herein referred to as "theatrical optical discs." Theatrical optical discs are similar to consumer digital video discs (DVD) which are now widely available. Like consumer DVDs, theatrical optical discs provide dense storage of digital information and are relatively inexpensive to produce while providing a high level of physical durability.

Double-sided dual-layer consumer DVDs hold approximately 15.96 gigabytes of information, allowing a two-hour movie to average 2.217 megabytes per second and still fit on a single DVD. Single-sided, single-layer consumer DVDs hold approximately 4.38 gigabytes, limiting a two-hour movie to an average of 608 kilobytes per second. Theater-quality movies require approximately 78.6 megabytes of data per second. Assuming a single theatrical optical disc holds the same amount of data as a double-sided, dual-layer consumer DVD, a compression ratio of 36:1 is necessary to allow a single theatrical optical disc to hold an entire movie. Lower capacities, or lower compression ratios, require several discs to hold a single theater-quality movie.

Coupled with the storage media 114 is a tamper-proof identification system 116. The tamper-proof identification system allows information to be transferred to media players 118 without reading the storage media 114. Many different identification systems are available. The

desired characteristics of the identification system are low cost, read/write capability, and the capability to accurately interrogate one device in the presence of other devices without the need for direct contact. One identification system that meets these criteria is the Texas Instruments Registration and Identification System (TIRIS®) which is capable of storing digital information and transmitting that information when exposed to an RF energy source. The remainder of this disclosure will assume the identification system is a TIRIS® module.

The TIRIS transponder system, which is further disclosed in U.S. Patent 5,053,774 is comprised of two portions, an RF responder module 116 which is embedded in or attached to the object to be identified or tracked, and an RF module interrogator 122. In use, the RF interrogator 122 energizes the RF module 116 by irradiating the module with a beam of RF energy. The RF module 116 then emits an RF transmission in which information is encoded. The information includes the serial number of the RF module and additional information stored in the RF module 116. This additional information may be read out by the interrogator 122 or stored in the module 116 by the interrogator 122. Depending on the design of the RF module 116, the memory provided by the RF module 116 may be read-only memory, read/write memory, or write-once-read-many memory. Current TIRIS designs are available with at least 1024 bits of memory.

As shown by Figure 1, the first step in preparing optical media is digitally mastering 106 the source material 104. Typical theater images generally utilize display resolutions of between 1280 x 1024 and 2048 x 1024 pixels, with between 20 and 42 bits per pixel. At 24 frames per second, these resolutions require a data transfer rate between 0.629 and 2.11 gigabits per second-much too high to be cost effective. To lower the data rate and data storage requirements, the digital data must be compressed. Referring to Figure 1, the digitally mastered data is compressed 104, using any of the available image compression techniques.

Consumer DVD systems use MPEG2 digital data compression to reduce a two-hour movie to an average 4.7 megabits per second data rate. MPEG2, however, may not provide the high quality images required for large screen theaters. Other methods such as high bit rate MPEG and wavelet transforms are used by various embodiments. To further enhance security of the data, a non-consumer compression algorithm is chosen. The use of a non-consumer compression algorithm reduces the availability of decompression algorithms and circuitry and increases the effort and expense of defeating the disclosed security system.

Some embodiments of the disclosed invention add a digital watermark to the digital electronic cinema data prior to the compression step 108. A digital watermark is formed by changing some of the bits in an image. Ideally, a viewer will not be able to detect the changes in the image data, but when the image data is compared with the original image data the changed bits are evident. A digital watermark does not enhance security, but does provide traceability. Since each copy, or set of copies, of a motion picture has a unique watermark, any unauthorized copies seized are easily traced to the source. Alternative embodiments of the disclosed system insert watermark information as the media player 118 reads the electronic cinema data, or as the projector 128 processes and displays the data. Using multiple watermarks, added by the source, media player, and media projector, pinpoints where in the distribution chain an unauthorized copy of the data stream was made.

The compressed digital data is then encrypted 110 to prevent unauthorized access to the digitally mastered data. Although any encryption algorithm will suffice, the level of security will vary greatly depending on the algorithm chosen since some encryption techniques are much easier to defeat, or crack, than other encryption algorithms. For a given encryption technique, the length of the key, or code the receiver must know in order to decrypt the encrypted data,

66E70T-49802T60
5 determines the strength of the encryption since each bit added to the key length doubles the number of possible key words. To further enhance the strength of the encryption, one embodiment of the present invention changes the encryption algorithm or key within a given set of discs. For example, according to one embodiment of the present invention each of the theatrical optical discs required for a full-length motion picture uses a different encryption algorithm, and even portions of a single theatrical optical disc use different algorithms and keys. Assuming a sufficiently strong encryption technique is selected, once the digital data is encrypted, the information contained in the digitally compressed data is relatively safe from unauthorized duplication.

10 Once the digital electronic cinema data is compressed and encrypted, it is written to one or more storage devices 114, shown in Figure 1 as theatrical optical discs. At least one of the theatrical optical discs includes an identification module 116, typically an identification module such as a TIRIS module, which further increases the security of the distribution system. According to one embodiment, a TIRIS module is embedded in each of the theatrical optical
15 discs. The identification module 116 preferably is attached to or embedded in the media 114, but need only be associated with the media 114 to derive the benefits of the disclosed invention. For example, various embodiments of the disclosed invention foresee including the identification module 116 in the packaging material holding the media 114 and forming a separate cartridge with the identification module 116 which is sometimes even be shipped separately.

20 The identification module 116 is typically preloaded with several types of information, including information about the theatrical optical disc contents, information about the encryption algorithm used to encode the data, information about which media players and projectors are authorized to read and decode the information on the theatrical optical discs, and information

concerning the number of times the media may be used. According to various embodiments of the disclosed invention, the TIRIS module includes the key or keys necessary to decrypt the data on the theatrical optical discs. Including the decryption keys with the media, however, weakens the security of the overall system and is not preferred. Alternatives to including the decryption
5 keys with the media will be discussed below.

After the electronic cinema data is stored on the theatrical optical discs and the necessary information is stored in the identification module, the discs are shipped to the theaters. Since the theatrical optical discs are much smaller and lighter than the canisters of film previously used, and because the security techniques disclosed herein reduce or eliminate the need for in-transit
10 protection of the theatrical optical discs, theatrical optical discs produced according to the process shown in Figure 1 incur much lower shipping costs compared to corresponding canisters of film.

Once the storage media **114** are received by a theater, it is read by a media player **118** equipped with an identification module interrogator **122**. Although shown as two separate components in Figure 1, the media player **118** and projector **128** are combined as a single unit
15 according to some embodiments of the present invention. Alternative embodiments move some functions from one component to the other with various effects on the level of security provided by the system.

The identification module interrogator **122** reads the authorization data, or authorization code, from the identification module **116** located on the storage media **114** and compares the
20 authorization data to a unique identifier, such as the serial number, of the media player **118**. If the authorization data in the RF transponder **116** and the unique identifier agree, the media player **118** will read the media **114**. If the authorization data and the unique identifier do not match, the media player **118** does not read the media **114**. Requiring a match between the authorization data

and the media player 118 reduces or eliminates the value realized by the theft of the media 114 and therefore reduces the amount of physical security required to protect the media 114 during transit.

The authorization data contained in the identification module 116 and the media player's unique identifier need not be identical to be considered a "match." As long as there is a relationship between the authorization data and the unique identifier that allows the media player 118 to determine whether it is authorized, a match occurs when the media player 118 determines it is authorized to read the data from the media 114. For example, according to one embodiment a blank authorization code matches any identification code and authorizes all media players to read the media 114.

Alternative embodiments use multiple authorizations codes or special group authorization codes to authorize a group of media players to read the media 114. Including multiple authorization codes, or group codes, enables a data distributor to authorize all of the projectors at a particular theater, or chain of theaters, to read the media, granting the theater management flexibility to shift movies between screens based on ticket sales without the need to move equipment. Likewise, the use of a group code allows release of a title for viewing on home theater-class projectors, but not on commercial movie theater-class projectors--thus preserving the commercial market for royalty producing sales.

Assuming the media player authorization code matches the media player's unique identifier, the projector authorization code, which is also read from the identification module 116 embedded in the media 114, and the encrypted electronic cinema data read from the media 114 are sent by the media player 118 to the projector 128. The projector 128 compares the projector authorization code received from the media player 118 with the projector's unique identifier. If

the authorization code received from the media player matches the projector's unique identifier, the projector 128 will decrypt the electronic cinema data and decompress the decrypted data. The decompressed data, which is an exact copy of the digital master, is then displayed by the projector 128.

5 One of the major advantages of digital electronic cinema data is the ability of the data stream to describe itself. For example, headers in the electronic cinema data stream are used to describe the format of the electronic cinema data stream including the intended screen resolution, frame rate, and data word size, as well as the encryption and compression algorithms used. Once this information is known by the media player and projector, the electronic cinema data is
10 reformatted, if necessary, to optimize the display of the data on the screen. For this reason, the particular algorithms used and the particular design of the media player and projector are not critical to the implementation of the disclosed invention.

According to one embodiment of the disclosed invention, a digital light processing (DLP®) projection engine is used to display the electronic cinema data signal. To achieve a suitable image
15 quality for motion picture theater images, a three-chip digital micromirror device (DMD) design is envisioned, having a resolution of approximately 1280 x 1024 pixels or higher. Figure 2 is a block diagram of a three-chip DMD image projection system 200 capable of producing theater-quality true digital images. In Figure 2, a dichroic prism assembly 202 splits a beam of white light
20 204 from a light source 206 into three separate single-color light beams 208, 210, 212. Three DMDs 214, 216, 218 modulate these three single-color light beams and reflect the modulated light back to the prism assembly 202 where the modulated light is recombined into a full-color modulated light beam 220 and focused by lens 222 onto a projection screen (not shown). Prism assembly 202 is typically comprised of several individual prisms which have dichroic filters on

various surfaces and which utilize total internal reflection to separate certain wavelengths of light from the remainder of the light beam.

One feature of the system of Figure 1, which further increases the difficulty of defeating the security system, is that decrypted data is never available at any connector external to the projector unit **128** or media player **118**. Some embodiments of the projector **128** include display devices **138** which are integrated on a single integrated circuit with the decompress/format functions **134** and memory **136** so that the decrypted data is not even available outside an integrated circuit. Preventing access to the decrypted data prevents owners and users of projector **128** from recording the decrypted information during a playback of the recorded material.

As discussed above, a decryption code, or key, is crucial to the efficient decryption and playback of the media **114**. Therefore, the transmission of the key from the media producer, typically the production studio, to the media user, typically the theater, adds another dimension to the strength of the security measures. The simplest method of providing the key to the theater is to simply include the key with the media **114**, either as part of the data recorded on the media **114** or as part of the security codes written into the identification module **116**. Since the key is provided to whoever gains possession of the media **114**, this approach relies only on the authorization codes sent with the media **114**, and the design of the media players **118**, to prevent unauthorized access to the recorded data.

Data security is enhanced by transmitting the key to the media player **118** through a separate distribution channel. According to various embodiments of the present invention, copies of the encryption key are sent to the media player **118** through various other channels including the U.S. Postal Service or other mail carrier, dial-up or on-line telecommunication links, and

direct satellite broadcasts. Each of these communications channels is utilized autonomously by the media player **118**, or independently by a projectionist.

In addition to providing increased data security, the disclosed security system also provides a convenient means for collecting information regarding media usage by the theaters.

- 5 The type of information collected from the theaters is limited only by the imagination, but will generally deal with the types of information that effect either the royalties paid by the theaters or the marketing strategies of the distributors. Such information will be referred to as usage information for the purposes of this disclosure.

- 10 For example, the identification module interrogator **122** may store usage information about how many times a particular disc has been read, or when the disc was read, in the identification module **116** embedded in the media **114**. If more than one projector **128** or media reader **118** is authorized to read the media **114**, the identification module interrogator **122** may store usage information about which media player **118** or projector **128** actually did read the media **114** in the identification module's memory. Usage information concerning the time and
15 date of the showing, or the number attending the showing could also be stored in the identification module **116**.

- All of the usage information stored by the theaters during the use of the media **114** may be read by an information collection agency upon return of the media **114**. Information collection agencies include the motion picture studios, distributors, theaters, or marketing agencies. The
20 usage information is used to determine royalty and other payments owed by or to the theaters, advertising agencies, or other entities, and possibly to refine marketing strategies for future releases. By storing the usage information in the identification module **116** instead of on the media **114** itself, the usage information can be read even if the media **114** intentionally is

destroyed prior to return shipment to the distributor. Destruction of the media **114** prior to reshipment eliminates the risk of theft since the media **114** would be of no value to potential thieves.

Alternatively, the usage information is transferred to the information collection agency by the media player **118** or projector **128** using a wired or wireless communications link. For example, the media player **118** or projector **128** may use a dial-up service, internet access, or a satellite link to transmit the information to the information collection agency.

An additional level of security is provided by packaging the media **114** in a tamper-proof cartridge **302** as shown in Figure 3. The tamper-proof cartridge **302** is designed to prevent unauthorized access to the media **114**. A first cartridge design prevents the cartridge **302** from being opened except by a media player **304**. This design is further strengthened by designing the media player **204** to open cartridges **302** only after receiving the proper authorization code from the media's identification module **116** or a separate cartridge identification module **310**. A second cartridge design includes a separate authentication means within the cartridge **302** which will not allow the cartridge **302** to be opened unless the authentication means receives the proper code from the media player **304**. In addition to merely preventing the cartridges **302** from opening, some embodiments of the tamper-proof cartridges **302** damage or destroy the media **114** contained within the cartridge **302**. For example, various embodiments damage the media by dyeing, scratching, or breaking the media **114**, or by erasing the data stored in the identification system module, including the encryption key if stored in the identification system module.

The media player/projector **308** shown in Figure 3 also provides a separate input for video signals. These video signals bypass the decryption and decompression blocks and are merely reformatted for display on the DLP projection engine. Alternative embodiments route the

alternate video inputs through the decryption and decompression blocks as needed. The alternate video path is used for video sources which are incompatible with the media 304. For example, a theater can show a pay-per-view boxing match to patrons using a separate video receiver and the alternate video signal path.

5 The media player/projector 308 shown in Figure 3 also includes outputs from the system controller which enable the player/projector 308 to control other theater equipment. According to one embodiment, the player/projector dims the lights and opens the theater curtain as a movie starts. Additionally, the player/projector is capable of projecting commercial, previews, and trailers selected by the local theater before and after a movie showing, without the need for
10 operator intervention.

 Thus, although there has been disclosed to this point a particular embodiment for system for the secure transmission of digital data, and method therefore, which greatly increases the distributor's control over access to the digital data, it is not intended that such specific references be considered as limitations upon the scope of this invention except insofar as set forth in the
15 following claims. Furthermore, having described the invention in connection with certain specific embodiments thereof, it is to be understood that further modifications may now suggest themselves to those skilled in the art, it is intended to cover all such modifications as fall within the scope of the appended claims.

WHAT IS CLAIMED IS:

1. A secure digital image projection system having at least one identification code identifying said image projection system, said image projection system comprising:
 - an identification system interrogator for reading an authorization code from an identification system module associated with a data storage medium;
 - a verification unit for verifying said authorization code matches said identification code;
 - a media player for reading digital data stored on said data storage medium; and
 - a projection unit for displaying said digital data on the condition that said authorization code matches said identification code.
2. The secure digital image projection system of Claim 1, said identification system module comprising an RF identification system module.
3. The secure digital image projection system of Claim 1, said identification system module comprising a TIRIS transponder.
4. The secure digital image projection system of Claim 1, wherein said digital data stored on said medium is encrypted, said projection system further comprising:
 - a decryption unit for decrypting said encrypted digital data prior to display of said digital data.
5. The secure digital image projection system of Claim 1, said image projection system further comprising:
 - a media jukebox for opening a tamper-proof cartridge containing said data storage medium, and for accessing said data storage medium.

6. The secure digital image projection system of Claim 1, wherein said projection system adds a digital watermark to said digital data read from said data storage medium.
7. The secure digital image projection system of Claim 1, wherein said media player adds a digital watermark to said digital data read from said data storage medium.
8. The secure digital image projection system of Claim 1, wherein said projection unit adds a digital watermark to said digital data read from said data storage medium.
9. The secure digital image projection system of Claim 1, wherein said projection system stores usage information on said identification system module.
10. The secure digital image projection system of Claim 9, wherein said usage information comprises at least one said identification code identifying said image projection system.
11. The secure digital image projection system of Claim 1, wherein said projection system transmits usage information to a collection agency.
12. The secure digital image projection system of Claim 11, wherein said usage information comprises at least one said identification code identifying said image projection system.
13. The secure digital image projection system of Claim 1:
 - said media player having a first identification code;
 - said projector unit having a second identification code; and
 - said verification unit comprising a first verification unit in said media player and a second verification unit in said projector unit, said authorization code comprising a first and a second authorization code, said media player only reading said digital data from said data storage medium on the condition that said first authorization code matches said first identification code, and said projector unit only displaying said digital data on the condition that said second authorization code matches said second identification code.

14. A secure digital data media player comprising:

an identification system interrogator for reading authorization information from an identification system module attached to a digital data storage medium and verifying said authorization information authorizes said media player to read said digital data storage medium; and

a media reader for reading data from said digital data storage medium and outputting said data on the condition said authorization information authorizes said media player to read said digital data storage medium.
15. The secure digital data media player of Claim 14, said identification system module comprising an RF identification system module.
16. The secure digital data media player of Claim 14, said identification system module comprising a TIRIS transponder.
17. The secure digital data media player of Claim 14, wherein said digital data stored on said medium is encrypted, said media player-projector further comprising:

a decryption unit for decrypting said encrypted digital data prior to display of said digital data.
18. The secure digital data media player of Claim 14, further comprising:

a media jukebox for opening a tamper-proof cartridge containing said data storage medium, and for accessing said data storage medium.
19. The secure digital data media player of Claim 14, wherein said media player adds a digital watermark to said data read from said digital data storage medium.
20. The secure digital data media player of Claim 14, wherein said media player adds a digital watermark to said data read from said digital data storage medium.

21. The secure digital data media player of Claim 14, wherein said projection system stores usage information on said identification system module.
22. The secure digital data media player of Claim 21, wherein said usage information comprises at least one said identification code identifying said secure digital data media player.
23. The secure digital data media player of Claim 14, wherein said projection system transmits usage information to a collection agency.
24. The secure digital data media player of Claim 23, wherein said usage information comprises the at least one said identification code identifying said secure digital data media player.
25. A secure data storage medium comprising:
 - a digital storage medium for storing digital data; and
 - an identification system module corresponding to said digital storage medium, said identification system module containing an authorization code describing which media players are authorized to read digital data from said digital storage medium.
26. The secure data storage medium of Claim 25, said digital storage medium comprising an optical disc.
27. The secure data storage medium of Claim 25, said identification system module comprising a TIRIS transponder.
28. The secure data storage medium of Claim 25, said identification system module comprising a TIRIS transponder.
29. The secure data storage medium of Claim 25, wherein said identification system stores usage information.

30. The secure data storage medium of Claim 29, wherein said usage information comprises information concerning the number of time said digital data has been read.
31. A method of securely distributing digital data, said method comprising:
 - writing digital data onto a digital storage medium;
 - attaching an identification system module to said digital storage medium, said identification system module containing an authorization code indicating which media readers are authorized to read said digital storage medium; and
 - transferring said digital storage medium to a user.
32. The method of Claim 31, said writing step comprising the step of writing digital data onto an optical disc.
33. The method of Claim 31, said attaching step comprising the step of attaching an RF identification system to said digital storage medium.
34. The method of Claim 31, said attaching step comprising the step of attaching a TIRIS responder to said digital storage medium.
35. The method of Claim 31, further comprising the step of:
 - adding a digital watermark to said digital data; and
 - wherein said step of writing digital data onto a digital storage medium comprises the step of writing said digital data containing said digital watermark onto said digital storage medium.
36. The method of Claim 31, further comprising the step of:
 - reading said digital data from said digital storage medium; and
 - storing usage information on said digital storage medium.
37. The method of Claim 31, further comprising the step of:

reading said digital data from said digital storage medium; and
transmitting usage information to a collection agency.

38. A method of tracking the use of information, said method comprising:
storing said information on storage media;
reading said information;
storing usage information concerning said reading step on said storage media; and
transmitting said information to an information collection agency.
39. The method of Claim 38 wherein said storing usage information step comprises:
storing usage information concerning said reading step in an identification system
module attached to said storage media.
40. The method of Claim 39 wherein said transmitting said information step comprises:
transferring said identification system to a distributor.
41. The method of Claim 39 wherein said transmitting said information step comprises:
transferring said identification system to a distributor.
42. The method of Claim 39 wherein said transmitting said information step comprises:
transferring said identification system to a distributor.

ABSTRACT

A secure digital data distribution system (100) for preventing unauthorized access to digital data. The system utilizes an identification system module (116) embedded in a digital storage media (114) to grant authorization to media players (118). Prior to reading the digital data recorded on the media (114), an identification system interrogator (122) reads authorization data from the identification system module (116) to determine whether the media player (118) is authorized to read the media (114). If the authorization data matches the media player's unique identifier, authorization is granted and the media player (118) commences to read the media (114).

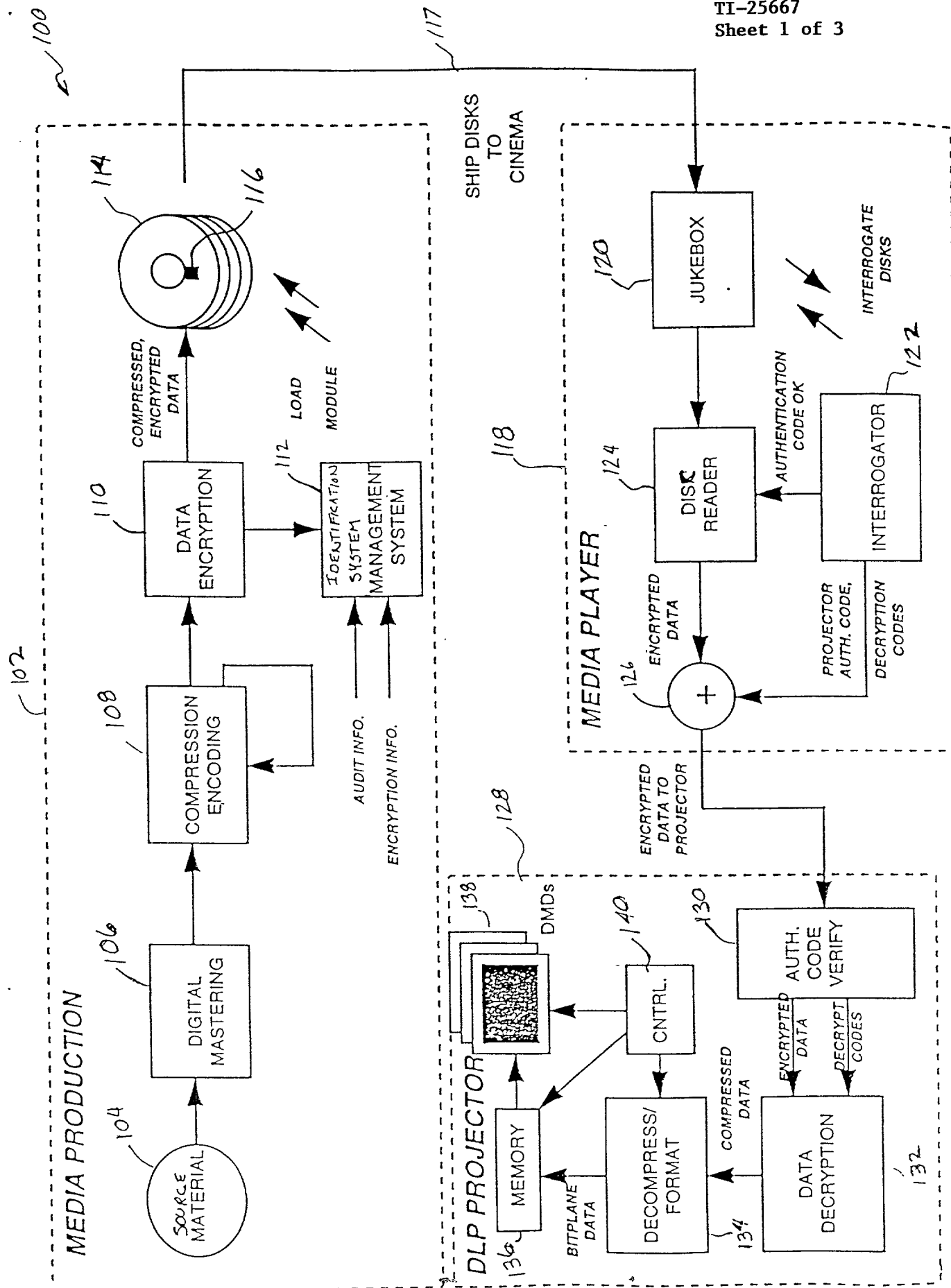


Figure 1.

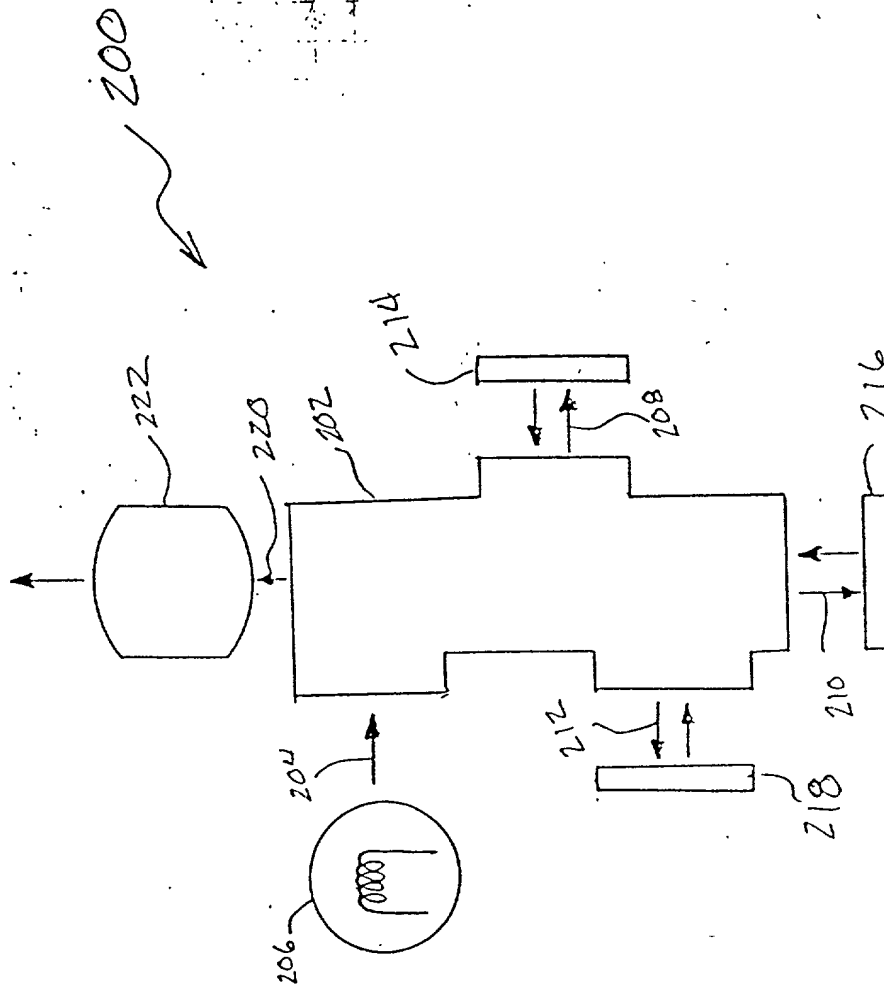


FIGURE 2

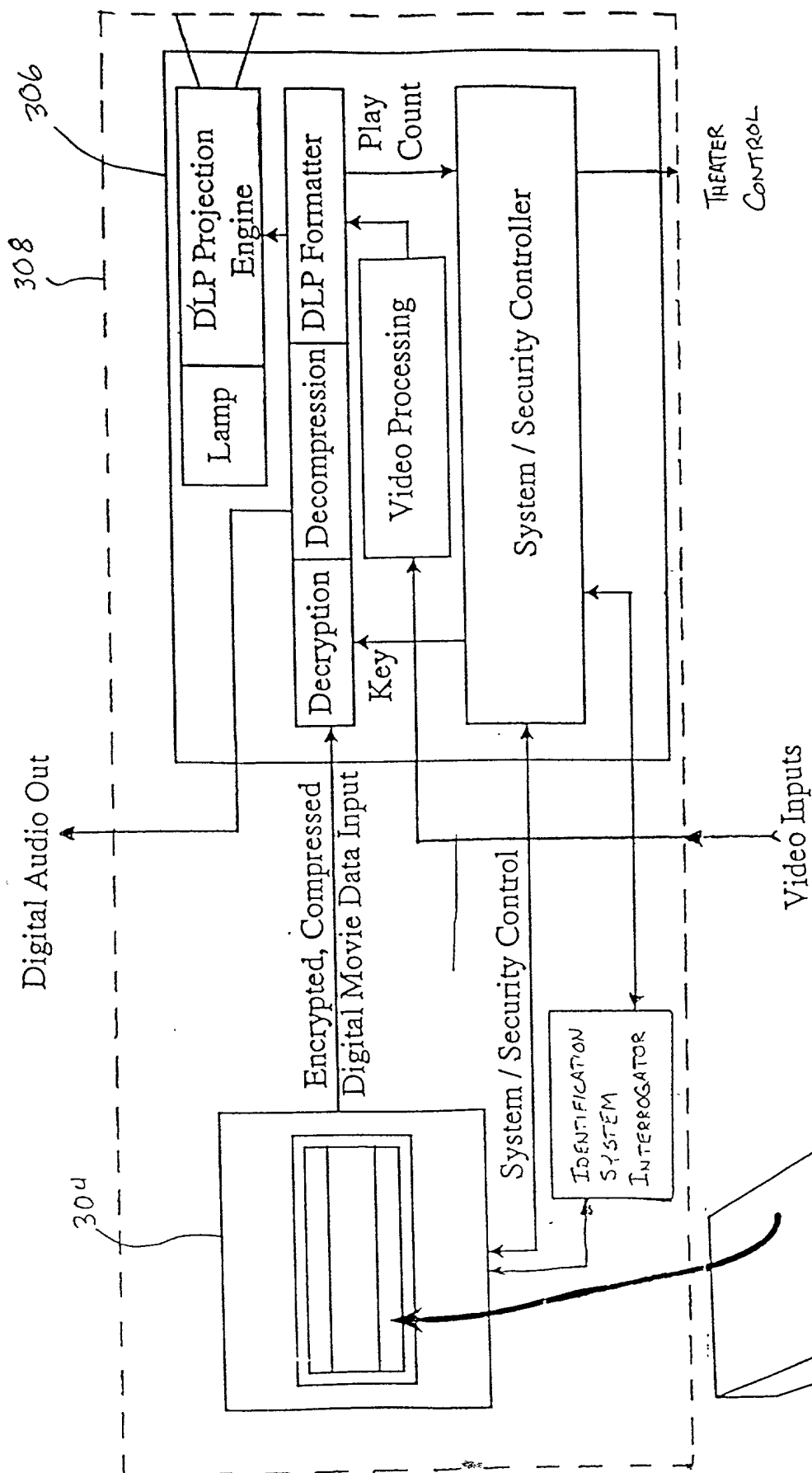
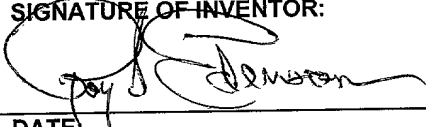
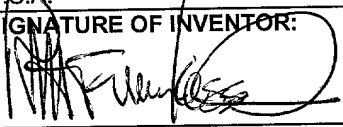
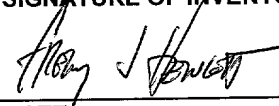


FIGURE 3

APPLICATION FOR UNITED STATES PATENT DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I declare that my residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am the original, first and sole inventor if only one name is listed below, or an original, first and joint inventor if plural inventors are named below, of the subject matter which is claimed and for which a patent is sought on the invention entitled as set forth below, which is described in the attached specification; that I have reviewed and understand the contents of the specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration; that no application for patent or inventor's certificate on this invention has been filed by me or my legal representatives or assigns in any country foreign to the United States of America; and that I acknowledge my duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, section 1.56;

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

TITLE OF INVENTION:		
Secure Distribution Of Digital Data		
POWER OF ATTORNEY: I HEREBY APPOINT THE FOLLOWING ATTORNEYS TO PROSECUTE THIS APPLICATION AND TRANSACT ALL BUSINESS IN THE PATENT AND TRADEMARK OFFICE CONNECTED THEREWITH: Julie L. Reed, Reg. No. 35,349; James C. Kesterson, Reg. No. 25,882; Charles A. Brill, Reg. No. 37,786; Richard L. Donaldson, Reg. No. 25,673; William B. Kempler, Reg. No. 28,228; and Jay M. Cantor, Reg. No. 19,906		
SEND CORRESPONDENCE TO: Charles A. Brill Texas Instruments Incorporated P.O. Box 655474, M/S 3999 Dallas, Texas 75265		DIRECT TELEPHONE CALLS TO: Charles A. Brill (214) 917-4378
NAME OF INVENTOR: (1)	NAME OF INVENTOR: (2)	NAME OF INVENTOR: (3)
Roy I. Edenson	Peter F. van Kessel	Gregory J. Hewlett
RESIDENCE & POST OFFICE ADDRESS: 404 Apollo Court Richardson, Texas 75081	RESIDENCE & POST OFFICE ADDRESS: 1311 San Mateo Dr. Allen, Texas 75013	RESIDENCE & POST OFFICE ADDRESS: 700 Lower State Rd., #16-A1 520 Skippack Pike Horsham Township Blue Bell, PA North Wales, Pennsylvania 19454 19422
COUNTRY OF CITIZENSHIP: U.S.A.	COUNTRY OF CITIZENSHIP: U.S.A.	COUNTRY OF CITIZENSHIP: (MONTGOMERY County) U.S.A. <i>PH</i>
SIGNATURE OF INVENTOR: 	SIGNATURE OF INVENTOR: 	SIGNATURE OF INVENTOR: 
DATE: 7/22/98	DATE: 7/23/98	DATE: 7/22/98

TITLE OF INVENTION:

Secure Distribution Of Digital Data

POWER OF ATTORNEY: I HEREBY APPOINT THE FOLLOWING ATTORNEYS TO PROSECUTE THIS APPLICATION AND TRANSACT ALL BUSINESS IN THE PATENT AND TRADEMARK OFFICE CONNECTED THEREWITH:

Julie L. Reed, Reg. No. 35,349; James C. Kesterson, Reg. No. 25,882; Charles A. Brill, Reg. No. 37,786; Richard L. Donaldson, Reg. No. 25,673; William B. Kempler, Reg. No. 28,228; and Jay M. Cantor, Reg. No. 19,906

SEND CORRESPONDENCE TO:

Charles A. Brill
Texas Instruments Incorporated
P.O. Box 655474, M/S 3999
Dallas, Texas 75265

DIRECT TELEPHONE CALLS TO:

Charles A. Brill
(214) 917-4379

NAME OF INVENTOR: (1)

Paul S. Breedlove
Paul S. Breedlove

NAME OF INVENTOR: (2)

William B. Werner

NAME OF INVENTOR: (3)

Keith H. Elliott

RESIDENCE & POST OFFICE ADDRESS:

2703 Lakeside
McKinney, Texas 75070

RESIDENCE & POST OFFICE ADDRESS:

3113 Hoffman Drive
Plano, Texas 75025

RESIDENCE & POST OFFICE ADDRESS:

5200 Englenook Court
Plano, Texas 75023

COUNTRY OF CITIZENSHIP:

U.S.A.

COUNTRY OF CITIZENSHIP:

U.S.A.

COUNTRY OF CITIZENSHIP:

U.S.A.

SIGNATURE OF INVENTOR:

Paul S. Breedlove

SIGNATURE OF INVENTOR:

William B. Werner

SIGNATURE OF INVENTOR:

Keith H. Elliott

DATE:

July 23, 1998

DATE:

7/23/98

DATE:

7/23/98